NEDERLANDSE ORDE VAN ADVOCATEN

0 BD

Aan de Minister van Veiligheid en Justitie
De heer mr. I.W. Opstelten
Postbus 20301
2500 EH DEN HAAG

Den Haag, 28 augustus 2014
Dossiernummer:
Doorkiesnummer:
Faxnummer:
E-mail:

Betreft: Aanvullende consultatie conceptwetsvoorstel computercriminaliteit III

Zeer geachte heer Opstelten,

Bij brief van 11 juli jl. heeft u de Nederlandse orde van advocaten verzocht te adviseren over het conceptwetsvoorstel computercriminaliteit III.

De algemene raad heeft het conceptwetsvoorstel voorgelegd aan zijn adviescommissie strafrecht. In 2013 heeft de adviescommissie al advies uitgebracht over dit onderwerp en de commissie persisteert nadrukkelijk bij de in 2013 geuite bezwaren. Het advies van 10 juli 2013 treft u daarom aan als bijlage bij deze brief.

Met betrekking tot de uitbreiding ten behoeve van de zogenoemde lokpuber heeft de adviescommissie nog één aanvullend, meer principieel bezwaar op het gebied van systematiek. Gelet op de toelichting in de hernieuwde memorie van toelichting gaat het hier in wezen om het mogelijk maken van een bepaalde opsporingsmethode. Dat behoort volgens de commissie plaats te vinden door een aanpassing van strafvordering, maar gebeurt hier door een aanpassing van het materiële strafrecht. De adviescommissie strafrecht maakt hiertegen bezwaar.

De algemene raad sluit zich aan bij de overwegingen van de adviescommissie en verzoekt u deze bij de verdere voorbereiding van het wetsvoorstel te betrekken.

Met de meeste hoogachting,
namens de algemene raad,

algemeen secretaris

Bijlage

Bezoekadres
Neuhuyskade 94
2596 XM Den Haag
Tel. 070 - 335 35 35
Fax 070 - 335 35 31

Postadres
Postbus 30851
2500 GW Den Haag

www.advocatenorde.nl

NEDERLANDSE ORDE VAN ADVOCATEN

Van	:	*Adviescommissie Strafrecht*
Datum	:	10 juli 2013
	:	
Betreft		**Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)**

SAMENVATTING

Conclusie

De Adviescommissie Strafrecht (ACS) heeft fundamentele bezwaren tegen de invoering van de bevoegdheid om heimelijk op afstand in een geautomatiseerd werk binnen te kunnen dringen (art. 125ja Sv) en het voorgestelde decryptiebevel (art. 125k Sv) . Met betrekking tot de invoering van de nieuwe bevoegdheden van het ontoegankelijk maken van gegevens (art. 126p Sv) en de strafbaarstelling van het overnemen en de heling van gegevens (art. 136c en 139f Sv) stelt de ACS concrete wijzigingen ter verbetering voor.

Kernpunten

Het wetsvoorstel beslaat een vijftal onderwerpen. In deze samenvatting worden per onderwerp puntsgewijs het commentaar van de ACS opgesomd.

1. Commentaar op de invoering van het heimelijk binnendringen (art. 125ja Sv):
   - De invoering van de voorgestelde bevoegdheid is een zeer verstrekkende verdere stap in de verruiming van de mogelijkheden om burgers heimelijk te bespieden, terwijl uit de toelichting bij dit wetsvoorstel niet kan worden afgeleid waar nu precies de noodzaak ligt om deze vergaande maatregelen door te voeren. Er worden immers geen concrete noch cijfermatige voorbeelden gegeven van zaken die door een gebrek aan bevoegdheden zouden zijn "misgegaan". In de concept MvT wordt bij herhaling het voorbeeld van kinderpornografie aangehaald, maar dat is minst genomen misleidend, omdat de voorgestelde bevoegdheid niet beperkt is tot dat type zaken, maar ook toepasbaar is bij zulke buitengemeen ernstige vormen van criminaliteit als herhaalde winkeldiefstal of – onder omstandigheden – het benadelen van de gezondheid of welzijn van een dier. Zonder deugdelijke onderbouwing is de ACS van oordeel dat een dergelijk vergaand opsporingsmiddel niet zou moeten worden ingevoerd. Derhalve wijst de ACS de introductie van het heimelijk binnendringen in zijn geheel af.
   - Bij wijze van subsidiaire bezwaren voert de ACS nog aan dat
     - in ieder geval de voorgestelde toepassingsvoorwaarden (kort gezegd: feit van art. 67 Sv en ernstige inbreuk op de rechtsorde) te ruim zijn. Nadere inperking tot specifieke delicten en/of beperking tot situaties waarin sprake is van lichamelijk letsel, levensgevaar of gevaar voor de vrijheid van personen of gemeen gevaar voor goederen dat een bedreiging voor het voortbestaan van de staat of de mensheid oplevert;
     - regels van rechtsmacht zich tegen de bevoegdheid verzetten. Op dit moment wordt binnen de Raad van Europa gediscussieerd over gegevensvergaring over de landsgrenzen heen – het is aangewezen deze discussie eerst af te wachten alvorens in Nederland alvast dergelijke vergaarde bevoegdheden te introduceren waarbij territoriale integriteit van andere staten moet wijken;
     - de formulering van art. 125ja lid 1 laatste deel eerste volzin Sv ("bij verdachte in gebruik") verhoudt zich slecht met de zin onder a ("het bepalen van de identiteit van de gebruiker". De ACS stelt in ieder geval voor deze laatste zin te schrappen;

- er niet alleen in de toelichting maar ook in de wettekst expliciet tot uitdrukking komt dat de bevoegdheid niet ziet op communicatie;
- de bevoegdheid bij invoering vraagt om een nieuwe c.q. herziene procedure in de wet omtrent het tappen/heimelijk binnendringen van gegevens van geheimhouders.

2. Commentaar op invoering ontoegankelijk maken gegevens (art. 126p Sv):
   - De voorgestelde tekst laat te veel ruimte om de bevoegdheid ook toe te passen in bagatelzaken. De ACS doet in dat opzicht een verbeterend tekstvoorstel;
   - De voorgestelde regeling, met de daaraan verbonden waarborgen zoals rechterlijke tussenkomst en toetsing, zouden een dode letter worden, indien niet ook ondubbelzinnig wordt vastgelegd dat voortaan bevelen tot het ontoegankelijk maken van informatie uitsluitend langs de weg van het voorgestelde art. 126p Sv kunnen worden gedaan.

3. Commentaar op invoering decryptiebevel (art.125k Sv):
   - Het rapport van de TILT is genuanceerder dan de Minister in de concept MvT doet voorkomen;
   - Het is de ACS niet duidelijk wat het nut en de noodzaak is om te komen tot een bevoegdheid die breekt met het huidige systeem dat een ontsleutelplicht in verband met nemo tenetur en het zwijgrecht niet aan de verdachte kan worden gericht;
   - Gelet op het ontbreken van duidelijke nut en noodzaak voor de praktijk, stelt de ACS voor om nu eerst te kiezen voor de minder vergaande optie, te weten een decryptieregeling conform de regeling van verhoor, dus met dezelfde normering als een verhoor (toegang tot een advocaat, cautie etc.).

4. Commentaar op strafbaarstelling van het maken van beeldopnamen in woning (art. 139e Sr):
   - Het voorgestelde art. 139e Sr is nergens toegelicht: daarmee is het nut, de noodzaak en de proportionaliteit niet inzichtelijk;
   - De huidige redactie roept meer vragen dan antwoorden op en lijkt strafbaar te stellen wat niet strafbaar gesteld zou moeten worden;
   - De bepaling is onder de maat en kan niet worden ingevoerd.

5. Commentaar op invoering strafbaarstelling overnemen en heling van gegevens (artt. 136c en 139f Sr):
   - Ter voorkoming van strafbaarstelling van feiten die niet strafbaar gesteld zouden moeten worden, stelt de ACS de strafbaarstelling art. 139f Sr slechts ziet op niet openbare informatie *"waarvan de betrokkene weet of redelijkerwijze moet vermoeden dat openbaarmaking of verspreiding een ernstige aantasting van de persoonlijke levenssfeer van een ander met zich zou brengen"*;
   - In de toelichting zou (nader) tot uitdrukking moeten komen wat de Minister precies onder *"algemeen belang"* in de zin van art. 139f lid 2 Sr verstaat;
   - De bepalingen zijn onduidelijk en in technische zin onder de maat en kunnen in de voorgestelde vorm niet worden ingevoerd.

Bijlage

Het volledige preadvies van de adviescommissie d.d. 10 juli 2013 (inclusief als bijlage het eerdere preadvies van de ACS d.d. 17 september 2010).

NEDERLANDSE ORDE VAN ADVOCATEN

Preadvies
van de Adviescommissie Strafrecht

inzake

het wetsvoorstel

Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

1. Inleiding

1.1 Het wetsvoorstel computercriminaliteit III strekt tot aanpassing van het Wetboek van Strafrecht en het Wetboek van Strafvordering op de volgende vijf onderwerpen:

1. De introductie van de opsporingsbevoegdheid om op afstand heimelijk in een geautomatiseerd werk binnen te dringen (heimelijk binnendringen);
2. De introductie van de opsporingsbevoegdheid tot het ontoegankelijk maken van gegevens op internet (ontoegankelijk maken gegevens);
3. De introductie van het decryptiebevel aan de verdachte (het decryptiebevel);
4. De strafbaarstelling van het maken van beeldopnamen in een woning of een andere niet voor publiek toegankelijke plaats (beeldopname in woning); en
5. De strafbaarstelling om wederrechtelijk van misdrijf verkregen gegevens over te nemen, voorhanden te hebben of bekend te maken (overnemen en heling van gegevens).

1.2 Over de onderwerpen 2, 3 en 5 is al eerder een wetsvoorstel ter consultatie ingediend (het wetsvoorstel computercriminaliteit II (TK 1998/1999, 26 671, nr. 2)). Geheel nieuw is onderwerp 1, de introductie van het op afstand heimelijk binnendringen in een geautomatiseerd werk. Kort gezegd wordt hiermee voorgesteld om aan politie en justitie de bevoegdheid te verlenen om computers en andere geautomatiseerde werken (zoals tablets en smartphones!) te kunnen (terug)hacken. Zonder nadere toelichting introduceert het wetsvoorstel voorts ook een nieuw luidend art. 139e Sr, de strafbaarstelling van het maken van (bijvoorbeeld) beeldopnamen in een woning of andere niet voor publiek toegankelijke plaats. Dit onderdeel wordt in de samenvatting van de concept Memorie van Toelichting (concept MvT) niet apart genoemd. De concept MvT gaat dus uit van vier (hoofd) onderwerpen. Aangezien de Adviescommissie Strafrecht (ACS) op dit onderdeel wel commentaar heeft, gaan wij in dit preadvies uit van vijf onderwerpen.

2. Heimelijk binnendringen – voorgestelde art. 125ja Sv

2.1 Het voorgestelde art. 125ja lid 1 Sv luidt:

"1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een opsporingsambtenaar als bedoeld in artikel 141, onder b, of een buitengewoon opsporingsambtenaar als bedoeld in artikel 142, eerste lid, onder b,

binnendringt in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager, bij de verdachte in gebruik, en met een technisch hulpmiddel onderzoek doet met het oog op:

a. het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker;

b. het overnemen van gegevens die in het geautomatiseerde werk of een daarmee in verbinding staande gegevensdrager zijn verwerkt, of die eerst na het tijdstip van afgifte van het bevel worden verwerkt, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;

c. de ontoegankelijkmaking van gegevens;

d. een bevel als bedoeld in de artikelen 126l, 126m, 126s, 126t, 126zf of 126zg;

e. een bevel als bedoeld in de artikelen 126g, 126o of 126zd, eerste lid, onder a."

In het belang van het onderzoek kunnen gegevens worden vastgelegd."

2.2 Hiermee wordt een zeer ingrijpende en vergaande opsporingsbevoegdheid geïntroduceerd. De ACS heeft fundamentele bezwaren tegen de invoering van deze bevoegdheid. Na uiteenzetting van deze bezwaren, zal er ook nog op meer detailniveau commentaar worden geleverd, het betreft dan in het bijzonder de hierboven onderstreepte passages.

Algemeen: (veel) te ruime bevoegdheid

2.3 Art. 125ja Sv creëert de bevoegdheid voor opsporingsambtenaren om op afstand met behulp van een technisch hulpmiddel in een geautomatiseerd werk binnen te dringen. Hoewel de techniek hierin telkens voortschrijdend zal zijn, kan nu al gedacht worden aan het heimelijk installeren van bepaalde softwareapplicaties (zie p. 26 concept MvT). Daarmee wordt het mogelijk gemaakt om gegevens af te tappen *"op het apparaat"* (zie p. 8 concept MvT), hetgeen voor de opsporing het voordeel oplevert dat de gegevens niet in versleutelde vorm worden aangetroffen, zoals dat volgens de concept MvT het geval is bij de huidige aftapmogelijkheden van art. 126m Sv (telefoon-, e-mail- en internettap) (zie p. 7 concept MvT). Bij de huidige tapmogelijkheden wordt niet het apparaat, maar de lijn (het telefoonnummer, het e-mailadres of het IP-adres) getapt. Daarmee ontstaan volgens de concept MvT gaten in de opsporing, bijvoorbeeld omdat de tap de gebruikmaking van bijvoorbeeld andere WiFi-netwerken niet dekt.

2.4 Volgens de voorgestelde bevoegdheid kan niet slechts worden binnengedrongen op het niveau van het apparaat, maar de voorgestelde bevoegdheid behelst tevens dat vanuit dat apparaat vervolgens alle gegevens worden bekeken en overgenomen die in *"een daarmee in verbinding staande gegevensdrager"* worden aangetroffen.

2.5 De voorgestelde bevoegdheid betreft aldus een enorme uitbreiding op de bestaande doorzoekings- en inbeslagnemingsmogelijkheden. De bestaande bepalingen zijn volgens de concept MvT onvoldoende dekkend omdat daarmee niet de gegevens worden bereikt die elders in een geautomatiseerd werk zijn opgeslagen, zoals een server op een andere plaats van doorzoeking of zelfs een ander land of op een onbekende of onbepaalde plaats zoals in een computercloud. Met het voorgestelde art. 125ja Sv kan volgens de concept MvT heimelijk worden binnengedrongen in *elk* geautomatiseerd werk, waar ter wereld dit werk ook maar gelokaliseerd is.

2.6 Het heimelijk binnendringen in een geautomatiseerd werk is een bevoegdheid die al kan worden toegepast door de AIVD en MIVD, zie meer in het bijzonder artt. 24-26 Wet op de Inlichtingen- en veiligheidsdiensten 2002 (WIV). Voor toepassing van de bevoegdheden van art. 24 WIV (binnendringen in geautomatiseerd werk), art. 25 WIV (gericht aftappen) en art. 26 WIV (ongericht aftappen) is telkens de toestemming van de Minister van Binnenlandse zaken en Koninkrijk relaties en/of de Minister van Defensie nodig.

2.7 Veiligheidsdiensten kunnen aldus bij aparte toestemming van de genoemde Minister(s) gebruik maken van deze vergaande bevoegdheid; het laat in ieder geval zien dat het om uitzonderlijke situaties dient te gaan. De ACS staat dan ook afwijzend om de bevoegdheid nu ook in het Wetboek van Strafvordering te introduceren, waardoor het instrument in veel breder bereik komt en niet alleen ziet op zaken waarbij de staatsveiligheid in het geding is. Deze afwijzende houding van de ACS is ook ingegeven tegen de achtergrond dat in Nederland per hoofd van de bevolking wereldwijd het meest gebruik maakt van telefoon- en gegevenstaps. Bij die stand van zaken kan niet verwacht worden dat van een terughoudend gebruik van de nieuwe bevoegdheid sprake zal zijn. Enkele cijfers illustreren de weinig vreugde scheppende koplopperspositie van ons land waar het de heimelijke bespieding van de communicatie van burgers betreft: Uit vrijgegeven cijfers blijkt dat in 2008 in Nederland door Justitie 26.425 tapbevelen voor mobiele en vaste telefoons zijn afgegeven. In de eerste helft van 2009 waren dat er 13.223. In deze cijfers zijn de afgegeven e-mail- en internettapbevelen niet meegerekend.

2.8 Als deze cijfers worden afgezet tegen de populatie van Nederland, is dat beschamend veel. Ter vergelijking: in de Verenigde Staten werden in 2008 1.891 tapbevelen afgegeven, bij een populatie van meer dan 300 miljoen. Verenigd Koninkrijk: 1.508 tapbevelen, populatie meer dan 60 miljoen. Frankrijk: 26.000 tapbevelen, populatie ongeveer 65 miljoen. Duitsland (cijfers 2007): 44.000 tapbevelen, populatie meer dan 80 miljoen. België (cijfers 2007): 3.603 tapbevelen, populatie ongeveer 11 miljoen.[1]

2.9 De ACS vraagt zich af of Nederland inmiddels niet is doorgeschoten in het veiligheidsdenken ten koste van waardevolle gemene goederen, zoals het recht op eerbiediging van de persoonlijke levenssfeer en de vrijheid van meningsuiting. De invoering van de voorgestelde bevoegdheid is een zeer verstrekkende verdere stap in de verruiming van de mogelijkheden om burgers heimelijk te bespieden, terwijl uit de toelichting bij dit wetsvoorstel niet kan worden afgeleid waar nu precies de noodzaak ligt om deze vergaande maatregelen door te voeren. Er worden immers geen concrete noch cijfermatige voorbeelden gegeven van zaken die door een gebrek aan bevoegdheden zouden zijn "misgegaan". In de concept MvT wordt bij herhaling het voorbeeld van kinderpornografie aangehaald, maar dat is minst genomen misleidend, omdat de voorgestelde bevoegdheid niet beperkt is tot dat type zaken, maar ook toepasbaar is bij zulke buitengemeen ernstige vormen van criminaliteit als herhaalde winkeldiefstal of – onder omstandigheden – het benadelen van de gezondheid of welzijn van een dier.[2]

---

[1] Bron: cijfers Nederland uit TK 2008-2009, 30517, nr. 13 (2008) en brief d.d. 10 november 2009 van Minister van Justitie aan Tweede Kamer, kenmerk 5608133/09 (eerste helft 2009). Andere informatie uit brief Bits of Freedom aan de Vaste kamercommissie voor Justitie d.d. 23 november 2009 (op internet beschikbaar) en Wikipedia wat betreft de populatie van België.

[2] Art. 36 Gezondheids- en welzijnswet voor dieren, via art. 122 van die wet en art. 67, 1e lid, onder c Sv.

2.10 Zonder deugdelijke onderbouwing is de ACS van oordeel dat een dergelijk vergaand opsporingsmiddel niet zou moeten worden ingevoerd. Derhalve wijst de ACS de introductie van het heimelijk binnendringen in zijn geheel af.

2.11 Bij wijze van subsidiaire bezwaren voelt de ACS zich evenwel genoodzaakt om ook op detailniveau commentaar op het wetsvoorstel te leveren.

(Veel) te ruime toepassingsvoorwaarden

2.12 Zoals gezegd, de bevoegdheid is niet beperkt tot de opsporing van kinderpornografie. Vereist is slechts een feit waarvoor op grond van art. 67 Sv voorlopige hechtenis is toegelaten en dat een ernstige inbreuk op de rechtsorde oplevert. Wij zeggen hier "slechts", omdat het exact dezelfde voorwaarden zijn die gelden voor de klassieke tapbevoegdheid van art. 126m Sv (voor telefoon, e-mail en internet). Gelet op de geschetste cijfers over 2008 en 2009 met betrekking tot het tapgedrag in Nederland hoeven we van die voorwaarden niet een al te grote filterende c.q. beschermende werking te verwachten.

2.13 Omdat de voorgestelde bevoegdheid echter veel verder gaat dan de bestaande tapmogelijkheden, pleit de ACS ervoor om, áls de bevoegdheid al wordt ingevoerd, de toepassing in ieder geval te beperken tot een aantal specifiek in de wet genoemde misdrijven, zoals bijvoorbeeld kinderpornografie en terrorisme. Ook zou gedacht kunnen worden aan een systeem zoals in Duitsland, waarbij de toepassing is beperkt tot de situatie waarin sprake is van 1) lichamelijk letsel, levensgevaar of gevaar voor de vrijheid van personen of 2) van gemeen gevaar voor goederen, dat een bedreiging oplevert voor het voortbestaan van de staat of de mensheid (zie p. 32 concept MvT voor bespreking van de situatie in Duitsland).

Rechtsmacht en Europese regelgeving

2.14 Onder kopje 2.8 "Onderzoek in een geautomatiseerd werk en rechtsmacht" van de concept MvT wordt stilgestaan bij de vraag hoe de nieuwe bevoegdheid zich verhoudt met het vraagstuk van rechtsmacht. De bevoegdheid schept immers de mogelijkheid om gegevens te bekijken en over te nemen, onafhankelijk van de vraag waar deze gegevens zich bevinden.

2.15 In de concept MvT (p. 35-36) wordt gewag gemaakt van een lopende discussie op Europees niveau, meer in het bijzonder binnen de Raad van Europa in het kader van de regeling van het zogenoemde Cybercrime Verdrag[3]. Opvallend is dat in de concept MvT wordt geconcludeerd dat art. 32 onder b van het Cybercrime Verdrag geen grondslag kan zijn voor de praktijk dat landen gegevens willen overnemen die in andere landen zijn opgeslagen. Verder blijkt dat er nog geen alternatieve regeling tot stand is gekomen. Gedacht wordt aan een Aanvullend Protocol bij het Cybercrime Verdrag waarin wordt *"voorzien in aanvullende regelgeving voor situaties waarin gegevens in verschillende jurisdicties zijn opgeslagen of waarin de fysieke locatie van de gegevens niet bekend is."* De paragraaf in de concept MvT eindigt met de zinsnede *"Deze maatregelen zouden in het Aanvullend Protocol bij het Cybercrime Verdrag vastgesteld kunnen worden"*.

[3] Convention on Cybercrime, Boedapest, Identificatienummer BWBV0001839, Trb. 2002, 18.

2.16 Hieruit volgt dat op dit moment geen internationale regelgeving bestaat, die toestaat dat een Staat gegevens mag overnemen uit werken die in zich een andere Staat bevinden. Dit gebrek aan internationale legitimiteit weerhoudt de Minister van Veiligheid en Justitie (de Minister) er echter niet van om in de concept MvT te concluderen dat *"wanneer de plaats van opslag van de gegevens niet bekend is, zelfstandig kan worden opgetreden. Maar het betekent ook dat als de plaats van opslag wel bekend is, zelfstandig optreden van de belanghebbende staat niet bij voorbaat is uitgesloten"* (p. 36 concept MvT). Kortom: als de plaats van opslag *niet* bekend is, dan mag Nederland zelfstandig optreden en als de plaats van opslag *wel* bekend is, dan mag Nederland ook zelfstandig optreden. De ACS wijst echter nogmaals op het ontbreken van internationale regelgeving die zo´n inbreuk op de erkende rechtmachts- en soevereiniteitsbeginselen zou kunnen legitimeren.

2.17 Gelet op het feit dat de discussie over gegevensvergaring en rechtsmacht thans nog in volle omvang binnen de Raad van Europa wordt gevoerd, lijkt het aangewezen de uitkomst van die discussie eerst af te wachten alvorens het standpunt in te nemen dat de territoriale integriteit van andere staten maar moet wijken voor het Nederlandse opsporingsbelang.

2.18 Op grond hiervan wordt voorgesteld in de bevoegdheid in ieder geval de beperking tot uitdrukking te brengen dat deze alleen kan worden toegepast als bekend is dat het geautomatiseerde werk in Nederland gelokaliseerd is.

"Bij verdachte in gebruik" vs. ter "bepalen van identiteit van de gebruiker"?

2.19 In paragraaf 2.5 van de concept MvT wordt onder het kopje *De verkennende fase* aangegeven dat eerst identificatie van het geautomatiseerde werk of van de verdachte die het geautomatiseerde werk gebruikt dient plaats te vinden. Die identificatie kan plaatsvinden door gebruikmaking van bestaande opsporingsbevoegdheden zoals het vorderen van verkeersgegevens (art. 126n Sv), het opvragen van gebruikersgegevens (art. 126na Sv) of het tappen van bijvoorbeeld het internetverkeer (art. 126m Sv). (p. 24 e.v. concept MvT). Pas ná deze verkennende fase kan de officier van justitie ervoor kiezen om daadwerkelijk in het geautomatiseerd werk binnen te dringen.

2.20 De ACS begrijpt dit zo, dat in de verkennende fase moet worden vastgesteld of de verdachte ook daadwerkelijk de gebruiker van het geautomatiseerde werk is waarin de opsporing wenst binnen te dringen. Zo leest de ACS ook het voorgestelde art. 125ja Sv lid 1: het geautomatiseerd werk waarin wordt binnengedrongen dient *bij de verdachte in gebruik* te zijn. Dit verhoudt zich echter slecht met het bepaalde in het voorgestelde art. 125ja lid 1 onder a Sv. Volgens deze voorgestelde bepaling is één van de toegelaten doeleinden voor het binnendringen *het bepalen van de identiteit van de gebruiker*. Deze doelomschrijving zou meebrengen dat het binnendringen van een geautomatiseerd werk al kan plaatsvinden voordat er (deugdelijk) onderzoek is gedaan naar de identiteit van de gebruiker. De vrees is reëel dat deze doelomschrijving in de praktijk zal worden aangewend om de bevoegdheid op apparaten of werken toe te passen, waarvan (nog) niet vaststaat dat zij door de of een verdachte worden gebruikt (vgl. de tapbevoegdheid van art. 126m Sv). Voor zover de voorgestelde bepaling inderdaad kan worden toegepast ter vaststelling van de identiteit (de bepaling is op dit punt in ieder geval tegenstrijdig c.q. onduidelijk), wijst de ACS deze mogelijkheid af.

2.21 Concreet wordt voorgesteld om de voorgestelde bepaling onder a in zijn geheel te schrappen, dan wel in ieder geval de woorden *"of het bepalen van de identiteit"* en de woorden *"de gebruiker"* te schrappen.

Het overnemen van gegevens vs. aftappen van communicatie

2.22 Uit de toelichting bij art. 126ja Sv blijkt duidelijk dat de bepaling onder b (het overnemen van gegevens) niet ziet op communicatie. De voorbeelden die worden genoemd zijn *"het vastleggen van afbeeldingen van kinderpornografie of van inloggevens van besloten "communities" of wachtwoorden waarmee de versleuteling van gegevens ongedaan kan worden gemaakt."*

2.23 De ACS stelt voor om deze duidelijke uitsluiting van communicatie ook in de wettekst op te nemen, zodat op dit (belangrijke) punt geen misverstanden kunnen ontstaan.

2.24 Voor het heimelijk aftappen en opnemen van communicatie of het opnemen van vertrouwelijke communicatie (het direct afluisteren), moet aldus worden teruggegrepen op de bestaande bevoegdheden in Titels IVa en V van het Wetboek van Strafvordering, meer in het bijzonder art. 126m Sv (telefoon-, e-mail- en internettap).

2.25 In het nieuwe art. 125ja onder d Sv wordt overigens wel een expliciete verbinding met de bestaande tap-bevoegdheden gelegd: het heimelijk binnendringen in een geautomatiseerd werk kan worden ingezet *met het oog op een tapbevel.* De voorgestelde volgorde lijkt dus te zijn: eerst binnendringen en daarna tappen. Gelet op het al besproken gegeven dat in Nederland door opsporingsinstanties naar verhouding veel gebruik wordt gemaakt van de bestaande tapbevoegdheden, vreest de ACS voor een praktijk waarbij vorderingen ex art. 125ja Sv standaard zullen worden gevolgd door vorderingen om te kunnen tappen. Door de combinatie van de oude tapbevoegdheden met de voorgestelde bevoegdheid tot heimelijk binnendringen kan het (privé)leven van iemand compleet in kaart worden gebracht. De ACS ziet dit – anders dan de huidige regering – niet als een zegen, maar als een beangstigend toekomstbeeld van hoe de komende generatie digitaal gestigmatiseerd kan raken, niet te vergeten ook op zeer jonge leeftijd.

Verschoningsrecht advocaten: van nummerherkenning naar apparaatherkenning

2.26 Voor tapkamers geldt inmiddels een systeem van nummerherkenning. Advocaten (en in de toekomst: andere wettelijke geheimhouders) geven hun telefoonnummers door, opdat deze bij de KLPD worden geregistreerd als geheimhoudernummers. Deze nummers kunnen niet getapt worden (behoudens in de uitzonderlijke omstandigheid dat de geheimhouder zelf als verdachte wordt aangemerkt). Deze blokkade geldt voor zowel uitgaand als ingaand telefoonverkeer (bellen en sms-en). Feitelijk is er sprake van een filter : zodra een nummer wordt herkend als geheimhoudernummer kan niet worden getapt.

2.27 De ACS stelt hierbij aan de orde dat deze procedure ook moet worden gewaarborgd bij de introductie van de nieuwe bevoegdheid tot binnendringen in een geautomatiseerd werk. Sterker nog, juist vanwege het diep ingrijpende karakter van de nieuwe bevoegdheid is het noodzakelijk dat het verschoningsrecht van geheimhouders met voldoende waarborgen wordt omkleed. In principe komt het er op neer dat niet alleen de nummers maar de geautomatiseerde werken c.q. apparaten van geheimhouders zouden moeten worden

herkend, opdat opspoorders zich geen heimelijke toegang tot vertrouwelijke geheimhouders documenten kunnen verschaffen. In elk geval ontbreekt in de voorgestelde bepalingen een regeling over de wijze waarop om moet worden gegaan met informatie en documenten die ook voor de opsporing geheim behoren te blijven. Gedacht kan bijvoorbeeld worden aan correspondentie tussen de verdachte en zijn raadsman, die op de computer van de verdachte wordt aangetroffen, en mogelijk op de voet van het voorgestelde art. 125ja lid 1 sub b. Sv uit het werk van de verdachte wordt "overgenomen". Een uitdrukkelijk in de wet voorgeschreven procedure voor dit soort situaties kan veel juridische procedures – en mogelijk mislukte vervolgingen door niet-ontvankelijkverklaringen – voorkomen.

3. <u>Ontoegankelijk maken gegevens – voorgesteld art. 126p Sv</u>

3.1 Het tweede onderdeel van het wetsvoorstel betreft de regeling van de bevoegdheid van de officier van justitie te vorderen dat gegevens op het internet ontoegankelijk worden gemaakt.

3.2 Het ontoegankelijk maken van gegevens werd al eens eerder voorgesteld, in het wetsvoorstel versterking bestrijding computercriminaliteit, ook wel het wetsvoorstel computercriminaliteit II genoemd (TK 1998-1999, 26 671, nr. 2) waarover de ACS op 17 september 2010 een preadvies uitbracht. Volledigheidshalve wordt dit preadvies als bijlage toegevoegd (<u>bijlage</u>). Toen was het belangrijkste bezwaar van de ACS het ontbreken van een rechterlijke toetsing en de mogelijkheid om aan de vordering van de officier van justitie een dwangsom te verbinden. Het nu voorliggende wetsvoorstel komt aan deze bezwaren tegemoet (zie p. 43 concept MvT).

3.3 Een belangrijk bezwaar uit het preadvies van 17 september 2010 blijft evenwel nog wel overeind. Het zij hierbij herhaald: volgens de voorgestelde tekst van artikel 125p Sv kan de vordering gedaan worden "*voorzover dit nodig is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.*" Deze redactie sluit niet uit dat een officier van justitie deze bevelsbevoegdheid gebruikt in een bagatelgeval, bijvoorbeeld een particuliere site waar één of slechts enkele auteursrechtschendende bestanden of hyperlinks zijn geplaatst. Gelet op het ingrijpende karakter van de bevoegdheid, en het altijd betrokken recht op vrije meningsuiting, kan dit niet de bedoeling van het wetsvoorstel zijn. Wetstechnisch is het echter van belang om bevoegdheden die slechts in serieuze gevallen zouden moeten worden gebruikt, ook uitdrukkelijk aan serieuze situaties te verbinden. De ACS stelt dan ook voor om in artikel 125p Sv toe te voegen "*indien dit dringend noodzakelijk is ter beëindiging van een strafbaar feit dat een ernstige inbreuk op de rechtsorde met zich brengt of ter voorkoming van nieuwe strafbare feiten die ernstige inbreuken op de rechtsorde met zich kunnen brengen*".

3.4 De huidige praktijk van het ontoegankelijk maken van informatie is, dat de politie of een officier van justitie een daartoe strekkend bevel geeft aan een provider, en met strafvervolging dreigt (wegens het niet voldoen aan een ambtelijk bevel dan wel op grond van medeplichtigheid of medeplegen aan een delict dat door of met de ontoegankelijk te maken informatie verband houdt, zoals heling of auteursrechtschending) voor het geval de provider niet aan het bevel voldoet. Deze praktijk wordt ook geschetst in de concept MvT, met name p. 44. De voorgestelde regeling, met de daaraan verbonden waarborgen zoals rechterlijke tussenkomst en toetsing, zouden een dode letter worden, indien niet ook ondubbelzinnig wordt vastgelegd dat voortaan bevelen tot het ontoegankelijk maken van

informatie uitsluitend langs de weg van het voorgestelde art. 126p Sv kunnen worden gedaan. Als de "informele" weg niet uitdrukkelijk wordt afgesloten, zal de "formele" weg van art. 126p Sv niet worden gebruikt.

4. **<u>Het decryptiebevel – voorgesteld art. 125k lid 4-7 Sv</u>**

4.1 Bij de invoering van de Wet computercriminaliteit I (1993) werd al een ontsleutelplicht (decryptiebevel) van gegevens ingevoerd (art. 125k Sv). Deze plicht kan niet aan een verdachte worden gericht.

4.2 Het voorstel om een decryptiebevel ter zake van gegevens ook aan de verdachte te kunnen richten is al onderwerp van discussie geweest bij de behandeling van het wetsvoorstel computercriminaliteit II. Destijds oordeelde de Minister naar aanleiding van de adviezen dat dit *"een stap te ver"* ging. De verklaringsvrijheid en het zwijgrecht waren in het geding (zie p. 48 concept MvT).

4.3 Deze duidelijke bewoordingen weerhouden de huidige Minister er niet van het zogenoemde decryptiebevel dat tegen de verdachte kan worden gericht in dit wetsvoorstel op te nemen in het voorgestelde art. 125k lid 4-7 Sv. Sterker nog, om het nieuwe bevel kracht bij te zetten wordt het niet meewerken bedreigd met een forse straf, te weten een maximale gevangenisstraf van drie jaar of een geldboete van de vierde categorie (nieuw art. 184b Sr).

4.4 De vraag is gerechtvaardigd wat er veranderd is, dat nu wel tot invoering van deze bevoegdheid zou moeten worden overgegaan. Dat een rapport van het Tilburg Institute for Law, Technology and Society van de Universiteit van Tilburg (TILT), genaamd *"Decryptiebevel en artikel 6 EVRM"*, niet uitsluit dat zo'n bevel in het licht van mensenrechtelijke verdragen houdbaar zal blijken, is immers geen reden om zo'n bevel in te voeren.

4.5 In het rapport worden 3 opties voorgesteld: A) handhaving van de huidige situatie, waarbij politie en justitie de verdachte kunnen verzoeken om vrijwillige medewerking, B) een decryptieregeling conform de regeling van het verhoor, dus met dezelfde normering als een verhoor (toegang tot een advocaat, cautie art. 29 Sv), en C) een decryptiebevel aan verdachten met strafbaarstelling van weigering.

4.6 De Minister heeft kennelijk voor optie C) gekozen. Daarbij is echter opmerkelijk dat de concept MvT beduidend stelliger is over de vraag of zo'n bevel "EHRM-proof" is dan het rapport van het TILT. Het rapport meldt over de keuze uit de 3 opties: *"De analyse van de EHRM-rechtspraak en het systeem van de Nederlandse wet wijst uit dat de tweede mogelijkheid [optie B], toevoeging ACS] te prefereren is boven de eerste mogelijkheid. Anders dan in 2000 hoeft de derde mogelijkheid echter niet op voorhand te worden afgewezen. Er is enige ruimte binnen de grenzen van het nemo-teneturbeginsel om een onder strafbedreiging afgedwongen ontsleutelplicht voor verdachten in te voeren. De effectiviteit daarvan zal gezien de zware eisen [die aan de toepassing gesteld moeten worden, toevoeging ACS] niet groot zijn, maar kan in incidentele gevallen wel aanwezig zijn."* Iets verder wordt door de rapporteurs precies de vrees van de ACS verwoord: *"De wetgever moet ook terughoudend zijn met een instrumentele inzet van het strafrecht; de bedoeling is immers om misdadigers te*

straffen voor feiten die zij hebben begaan, niet om verdachten te straffen voor het niet meewerken aan bewijsgaring."[4]

4.7 De ruimte voor optie C) is aldus beperkter dan de ontwerp MvT doet voorkomen. Daaraan doet niet af dat het voorstel voorziet in enkele (procedurele) waarborgen. Zo is het voorgestelde decryptiebevel alleen van toepassing op de specifieke delicttypen van kinderpornografie en terroristische misdrijven, en kan het bevel alleen door de officier van justitie en met voorafgaande schriftelijke machtiging van een rechter-commissaris worden gegeven. Het lijkt er op dat invoering van optie C) wordt voorgesteld, omdat het rapport de mogelijkheid tot zo'n encryptiebevel op een kier zet. Maar daarmee is nog niet de vraag beantwoord wat is het nut en de noodzaak van de voorgestelde regeling is, en waar die nut en noodzaak uit zouden kunnen blijken. In zowel het rapport van het TILT als in de concept MvT wordt verwezen naar de zaak Robert M. Maar onvermeld blijft daarbij dat juist in die zaak de verdachte gewoon *vrijwillig* heeft meegewerkt aan de ontsleuteling van gegevens. Voor die zaak was nu juist een encryptiebevel niet nodig, en werd het ontbreken van de mogelijkheid tot het geven van zo'n bevel ook niet gemist. Dat roept de vraag op naar (wel overtuigende) voorbeelden die rechtvaardigen dat voor de meest vergaande optie wordt gekozen.

4.8 De ACS stelt bij deze stand van zaken voor dat de eerste stap zou moeten zijn te kiezen voor de tussenvariant, dus optie B). Op deze wijze kan eerst worden bezien wat de effectiviteit is van een vrijwillig decryptiebevel. Pas als die uitkomsten aantoonbaar tot onaanvaardbare resultaten van het onderzoek leiden, kan optie C) alsnog worden overwogen.

---

[4] WODC Rapport *Het decryptiebevel en het nemo-teneturbeginsel*, Universiteit van Tilburg, BOOM Lemma uitgevers, 2012, p. 17-18.

5. Beeldopnamen in woningen – voorgesteld artikel 139e Sr

5.1 Het voorgestelde artikel 139e Sr luidt:

Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft degene die, gebruik makende van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of op een andere niet voor het publiek toegankelijke plaats, een afbeelding vervaardigt.

5.2 De concept MvT besteedt geen aandacht aan deze voorgestelde bepaling. De artikelsgewijze toelichting op artikel I, onderdeel D sluit niet aan bij de tekst van de bepaling. Zo moet worden vastgesteld dat deze voorgestelde bepaling in het geheel niet wordt toegelicht. Dat een toelichting op haar plaats is blijkt wel als wij de voorgestelde bepaling proberen toe te passen op enkel eenvoudige voorbeelden.

5.3 Hoe bijvoorbeeld te oordelen over beelden van beveiligingscamera's? Bijvoorbeeld in het geval van een vakantiewoning of tweede huis is het niet vreemd om binnenshuis camera's te plaatsen voor de periode dat de eigenaar afwezig is. Als zo'n beveiligingscamera een inbreker vastlegt, dan lijkt volgens de voorgestelde tekst de huiseigenaar strafbaar. Wat te doen met het in de Verenigde Staten zeer gebruikelijke verschijnsel van de "nanny-cam", een verborgen webcam waarmee de ouders toezicht kunnen houden op de taakvervulling van de persoon die kinderopvang aan huis levert? Wat is in dit verband een "*niet voor het publiek toegankelijke plaats*" ? Een clubhuis? Een school? Een kantoorgebouw? Een ministerie? Dekt deze bepaling eigenlijk wel het misbruik van webcams van derden, dat plaatsvindt door een inbraak in de computer van een ander, waarna op afstand de webcam van die andere computer aangezet kan worden? De webcam van de "gekraakte" computer is immers ter plaatse duidelijk aanwezig. Een laatste vraag is waarom dit feit, gezien zijn beperkte strafbedreiging, als misdrijf wordt gekwalificeerd. Waarom is het geen overtreding?

5.4 Zonder nadere toelichting zijn nut, noodzaak en proportionaliteit van de voorgestelde bepaling niet inzichtelijk.

6. Overnemen en heling van gegevens – voorgestelde artt. 136c en 139f Sr

6.1 Het laatste onderdeel van dit wetsvoorstel is de strafbaarstelling van het wederrechtelijk overnemen van gegevens en het daarover beschikken in de nieuw voorgestelde artt. 138c en 139f Sr (de zogenoemde overneming en heling van gegevens).

6.2 Zoals aangegeven, werd ook dit onderdeel eerder voorgesteld en ter consultatie ingediend. De bezwaren die in het toenmalige preadvies van 17 september 2010 door de ACS zijn opgeworpen gelden onverkort.

6.3 Het zij hierbij herhaald:

"Naar huidig recht zijn niet alle gegevens strafrechtelijk beschermd. Slechts geheime gegevens zijn beschermd. We kennen staatsgeheimen, we kennen gegevens die onder een bijzondere wettelijke geheimhoudingsplicht vallen (denk bijvoorbeeld aan de geheimhoudingsplicht die veel ambtenaren in wettelijke bepalingen hebben opgelegd

gekregen), of ook gegevens die werknemers onder zich hebben, en waarvoor zij een uitdrukkelijke geheimhoudingsverklaring hebben getekend. Naar huidig recht zijn niet-geheime niet-openbare gegevens niet strafrechtelijk beschermd. Met het voorliggende wetsvoorstel wordt daar verandering in aangebracht, nu strafbaar wordt gesteld het overnemen van niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk.

Ook hier lijkt de voorgestelde strafbaarstelling vooral ingegeven door de wens privacyschendingen door grootschalige internetverspreiding van niet-openbare gegevens te voorkomen. Maar ook hier is de strafbaarstelling zó ruim geformuleerd, dat daardoor ook allerlei maatschappelijk zeer aanvaardbare vormen van digitale kopieeractiviteiten worden gecriminaliseerd. Denk bijvoorbeeld aan de klokkenluider, die in de bedrijfscomputers bewijs voor corruptieve of mededingingsbeperkende afspraken vindt. Als deze burger dit bewijsmateriaal op een USB-stick zet en vervolgens aan de NMa of de rijksrecherche overhandigt, dan is deze burger onder de voorgestelde regeling strafbaar. Onder het voorgestelde artikel 139e Sr – dat verbiedt de "beschikking" te hebben over dergelijke niet-openbare gegevens – is vervolgens ook de NMa-ambtenaar of de rijksrechercheur die deze gegevens in ontvangst neemt (en er dus de beschikking over heeft), eveneens strafbaar. En ook de advocaat, die door een potentiële klokkenluider wordt ingeschakeld voor advies, wordt strafbaar zodra hij van zijn cliënt gekopieerd materiaal ontvangt.[5]

Ook hier kunnen weer legio voorbeelden worden gepresenteerd, die alle leiden tot de slotsom dat de aandacht van het wetsvoorstel te eenzijdig ligt op het voorkómen van de aantasting van de eer en goede naam door publicaties op het internet, en dat ter bescherming van dit (ook civielrechtelijk te handhaven) relatieve belang heel veel kind met heel weinig badwater wordt weggegooid.

De ACS meent dat ook hier aansluiting gezocht moet worden met de beledigingsbepalingen. In elk geval dient de voorgestelde verbodsbepaling te worden beperkt door toevoeging van bestanddelen: niet alle niet-openbare informatie zou moeten worden beschermd, maar – gelet op het voorbeeld in de toelichting – bijvoorbeeld slechts de niet-openbare informatie "waarvan de betrokkene weet of redelijkerwijze moet vermoeden dat openbaarmaking of verspreiding een ernstige aantasting van de persoonlijke levenssfeer van een ander met zich zou brengen". Dergelijke reikwijdtebeperkende bestanddelen zijn dringend gewenst, om de "collateral damage" van de voorgestelde bepaling te beperken."

6.4 De Minister reageert in de concept MvT als volgt op dit voorstel: *"Met betrekking tot de voorgestelde strafbaarstelling van het wederrechtelijk overnemen van gegevens is tijdens de consultatie van het eerdere conceptwetsvoorstel bepleit deze te beperken tot gegevens waarvan de dader weet of redelijkerwijs moet vermoeden dat openbaarmaking of verspreiding de persoonlijke levenssfeer kan schenden. Dit zou echter te beperkend zijn. Hoewel de persoonlijke levenssfeer een belangrijke doelstelling van het wetsvoorstel is, kunnen ook gegevens worden overgenomen uit overwegingen van geldelijk gewin zonder dat de schending van de persoonlijke levenssfeer daarbij aan de orde is."* (p. 67 concept MvT).

---

[5] Nu advocaten tuchtrechtelijk niemand mogen adviseren een strafbaar feit te begaan, kan het advies aan een potentiële klokkenluider overigens slechts zijn: "niet doen!, niets kopiëren!".

6.5 Voorts wordt naar aanleiding van de in de adviezen genoemde roep om verduidelijking van de term "wederrechtelijk" een extra lid voorgesteld in het nieuwe art. 139f Sr. Het voorgestelde lid 2 luidt: *"Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang bekendmaking van de gegevens vereiste."*

6.6 De vraag is of deze reactie en toevoeging voldoende tegemoet komt aan de geciteerde bezwaren. Wat de ACS betreft niet.

6.7 In de eerste plaats is de waarborg van art. 139f lid 2 Sr onvoldoende dekkend. Het dekt in het bijzonder niet de concrete voorbeelden die in het eerdere preadvies zijn genoemd (zie p. 3). De voorgestelde bepalingen stellen aldus nog steeds handelingen strafbaar die niet in het strafrecht thuishoren. De ACS stelt naar aanleiding van de reactie in de concept MvT op p. 67 voor om de toevoeging van de eerder door de ACS voorgestelde zinsnede over schending van de persoonlijke levenssfeer aan te vullen met de eenvoudige toevoeging *"en/of sprake is van persoonlijk winstbejag"* althans woorden van gelijke strekking (vgl. de wel gemaakte toevoeging in het voorgestelde art. 139f lid 1 onder b Sr.

6.8 In de tweede plaats is onduidelijk wat er precies onder *"algemeen belang"* moet worden verstaan. De toelichting geeft geen definitie en (be)noemt alleen de bekendmaking van journalisten en klokkenluiders die *"in het algemeen belang noodzakelijk is"*. Maar daarmee wordt al hetgeen vóór de bekendmaking is geschied – zoals het initiële overnemen van de gegevens door bijvoorbeeld een klokkenluider – niet gedekt, nu die uitsluiting alleen ziet op "de bekendmaking".

6.9 In de derde plaats is de toevoeging alleen van toepassing op de situatie van art. 139f Sr, de heling van gegevens. De toevoeging dekt dan ook name het (initiële) overnemen van belastend materiaal door een potentiële klokkenluider. Neem als voorbeeld de werknemer die bewijzen aantreft dat de onderneming waarin hij werkzaam is zich schuldig maakt aan ernstige vormen van criminaliteit (bijvoorbeeld systematische milieudelicten of omkoping), en die dat bewijsmateriaal overneemt om daarmee naar de politie te gaan. Ook deze werknemer is strafbaar onder het voorgestelde art. 138c Sr. De uitzondering van het voorgestelde art. 139f lid 2 Sr ziet immers alleen op de "bekendmaking". En omdat het materiaal met overtreding van het voorgestelde art. 138c Sr is verkregen, maakt een ieder die dat materiaal verwerft of "voorhanden heeft" (politie, advocaat, rechterlijke macht) zich schuldig aan "informatieheling" zoals strafbaar gesteld in art. 139f lid 1 onder a Sr. De uitzondering van het voorgestelde art. 139f lid 2 Sr ziet immers alleen op de "bekendmaking", en niet op het "voorhanden hebben". Dit eenvoudige voorbeeld geeft al aan dat de bepalingen in hun voorgestelde vorm onvoldoende onderscheidend zijn in maatschappelijk onwenselijk en geaccepteerd gedrag. Daarmee zijn zij in technische zin ondermaats en dienen zij in de voorgestelde vorm niet te worden ingevoerd.

7. <u>Conclusie</u>

7.1 De ACS constateert dat in het wetsvoorstel zonder voldoende grond of doordenking zeer vergaande en zeer ingrijpende bevoegdheden in het leven worden geroepen. De ACS maakt zich ernstig zorgen over de bepaald kritiekloze houding die de Minister ten aanzien van de digitalisering van de opsporing inneemt. Die zorgen worden versterkt door het feit dat juist in dit huidige tijdperk van smartphones, tablets, facebook en Skype een heel mensenleven digitaal eenvoudig zichtbaar is te maken. De algemene verontwaardiging naar aanleiding van

de onthullingen van de heer Snowden over de digitale bespiedingsactiviteiten van de Amerikaanse overheid raakt aan het onderwerp van het voorliggende wetsvoorstel. De verregaande digitalisering van het leven van burgers vraagt volgens de ACS niet om uitbreiding van het strafrecht, maar juist om terughoudendheid en zorgvuldiger proportionaliteitsafwegingen dan in het voorliggende wetsvoorstel zichtbaar zijn gemaakt.

Amsterdam, 10 juli 2013
Adviescommissie Strafrecht
mr. R. van der Hoeven, voorzitter,
namens deze, mr. R. Croes-Hoogendoorn, secretaris